REMARKS

Claims 1-26 remain in the present application. Claims 1, 10, 19, 21, 23 and 26 are amended herein. Applicants respectfully assert that no new matter has been added as a result of the claim amendments. Applicants respectfully request further examination and reconsideration of the rejections based on the arguments set forth below.

Claim Rejections – 35 U.S.C. §102

Claims 1-7, 9-11, 14, 21 and 23-24 are rejected under 35 U.S.C. §102(e) as being anticipated by United States Patent Number 6,704,872 to Okada (hereafter referred to as "Okada"). Applicants have reviewed the cited reference and respectfully assert that the embodiments of the present invention as recited in Claims 1-7, 9-11, 14, 21 and 23-24 are neither anticipated nor rendered obvious by Okada for the following reasons.

Applicants respectfully direct the Examiner to independent Claim 1 that recites a processor with secure cryptographic capabilities comprising (emphasis added):

> a digital secret comprising a secret key used in a key-based cryptographic process, wherein said digital secret is stored only within said processor, and <u>wherein said digital secret is operable to be used exclusively by said processor for both encryption and decryption</u>;
>
> a cryptography engine for performing said key-based cryptographic process internally within said processor, said cryptography engine operable to access said digital secret; and
>
> internal memory coupled to said cryptography engine for supporting said key-based cryptographic process.

Independent Claims 10 and 21 recite limitations similar to independent Claim 1. Claims 2-7, 10-11, 14 and 23-24 depend from their respective independent Claims and recite further limitations to the claimed invention.

Applicants respectfully submit that Okada fails to teach or suggest the limitations of "wherein said digital secret is operable to be used exclusively by said processor for both encryption and decryption" as recited in independent Claim 1. As recited and described in the present application, a digital secret is operable to be used exclusively by a processor for both encryption and decryption.

In contrast to the claimed embodiments, Applicants understand Okada to teach a secret key which is used by a software supplier *outside* of the processor for encryption and decryption. For example, Figure 3 of Okada teaches that a software supplier accesses the secret key and uses the secret key to encrypt data (col. 10, lines 15-34), thereby teaching that the use of the secret key is <u>not</u> exclusive to a processor as claimed. Additionally, page 2 of the rejection acknowledges this by stating that "access to the secret key by the software supplier is done externally to system 200." As such, assuming arguendo that a secret key as taught by Okada is analogous to a digital secret as claimed, Okada <u>teaches away</u> from the claimed embodiments by teaching a secret key which is *not* used exclusively by a processor instead of a digital secret used exclusively by a processor as claimed.

Additionally, in contrast to the claimed embodiments, Applicants understand Okada to teach a private key which is used only for decryption, and not encryption, within a processor. For example, Figure 4 of Okada teaches that a processor ID and software ID are encrypted by a software supplier using a public key and decrypted by processor 100 using a private key (col. lines 61-64; col. 12, lines 17-19). As such, Applicants respectfully assert that Okada fails to teach use of the private key for encryption within processor 100. Further, by

teaching that the processor ID and software ID which are eventually decrypted by processor 100 are encrypted by a software supplier external to processor 100, Okada teaches away from a digital secret used exclusively by a processor for encryption and decryption as claimed.

Applicants respectfully submit that Okada fails to teach or suggest the limitations of "wherein said internal memory is operable to perform state tracking associated with said key-based cryptographic process" as recited in Claims 4 and 23. As recited and described in the present application, an internal memory is operable to perform state tracking associated with a key-based cryptographic process.

In contrast to the claimed embodiments, Applicants fail to find any teaching or suggestion in Okada of an internal memory operable to perform state tracking associated with a key-based cryptographic process as claimed. As such, Applicants reiterate that Okada fails to teach or suggest the limitations of "wherein said internal memory is operable to perform state tracking associated with said key-based cryptographic process" as recited in Claims 4 and 23.

Applicants respectfully submit that Okada fails to teach or suggest the limitations of "wherein said cryptography unit comprises... said internal memory" as recited in Claim 6. As recited and described in the present application, a cryptography unit comprises an internal memory. The internal memory is coupled to the cryptography engine for supporting the key-based cryptographic process.

In contrast to the claimed embodiments, Applicants understand Okada to teach that ROM 14 is *outside of* and *separate from* encryption/decryption unit 17. For example, Figure 1 of Okada clearly shows that unit 17 does not comprise ROM 14. Assuming arguendo that ROM 14 as taught by Okada is analogous to an internal memory as claimed, and assuming arguendo that unit 17 as taught by Okada is analogous to a cryptography engine as claimed, Applicants reiterate that Okada fails to teach or suggest the limitations of "wherein said cryptography unit comprises... said internal memory" as recited in Claim 6.

Applicants respectfully submit that Okada fails to teach or suggest the limitations of "wherein said digital secret... is permanently and physically manifested within said processor" as recited in Claims 9 and 14. As recited and described in the present application, a digital secret is permanently and physically manifested within said processor.

In contrast to the claimed embodiments, assuming arguendo that the secret key taught by Okada is analogous to a digital secret as claimed, Applicants understand Okada to teach that the secret key is used by a software supplier *outside* of the processor as discussed above. Applicants respectfully assert that a secret key used *outside* of a processor is not permanently and physically manifested within the processor as claimed. Accordingly, Applicants reiterate that Okada fails to teach or suggest the limitations of "wherein said digital secret... is permanently and physically manifested within said processor" as recited in Claims 9 and 14.

Additionally, in contrast to the claimed embodiments, assuming arguendo that the private key taught by Okada is analogous to a digital secret as claimed,

Applicants fail to find any teaching or suggestion in Okada that the private key is permanently and physically manifested within said processor as claimed. Although Okada may teach that the private key is stored within processor 100 (col. 12, lines 18-19), Applicants respectfully assert that this does <u>not</u> amount to a teaching or suggestion that the private key is permanently and physically manifested within said processor as claimed. Accordingly, Applicants reiterate that Okada fails to teach or suggest the limitations of "wherein said digital secret... is permanently and physically manifested within said processor" as recited in Claims 9 and 14.

For these reasons, Applicants respectfully submit that independent Claim 1 is neither anticipated nor rendered obvious by Okada, thereby overcoming the 35 U.S.C. §102(e) rejection of record. Since independent Claims 10 and 21 recite limitations similar to those discussed above with respect to independent Claim 1, independent Claims 10 and 21 also overcomes the 35 U.S.C. §102(e) rejections of record. Since dependent Claims 2-7, 10-11, 14 and 23-24 recite further limitations to the invention claimed in their respective independent Claims, Claims 2-7, 10-11, 14 and 23-24 are also neither anticipated nor rendered obvious by Okada. Therefore, Claims 1-7, 9-11, 14, 21 and 23-24 are allowable.

<u>Claim Rejections – 35 U.S.C. §103</u>

<u>Claims 8, 13 and 22</u>

Claims 8, 13 and 22 are rejected under 35 U.S.C. §103(a) as being unpatentable over Okada in view of United States Patent Application Publication Number 2004/0098591 by Fahrny (hereafter referred to as "Fahrny"). Applicants have reviewed the cited references and respectfully submit that the

embodiments of the present invention as recited in Claims 8, 13 and 22 are not rendered obvious by Okada in view of Fahrny for the following reasons.

Applicants respectfully submit that Fahrny, either alone or in combination with Okada, fails to cure the deficiencies of Okada discussed above with respect to independent Claims 1, 10 and 21. Specifically, Fahrny fails to teach or suggest the limitations of "wherein said digital secret is internally accessible only within said processor." Consequently, since Claims 8, 13 and 22 recite further limitations to the invention claimed in their respective independent Claims, Claims 8, 13 and 22 are not rendered obvious by Okada in view of Fahrny. Thus, Claims 8, 13 and 22 overcome the 35 U.S.C. §103(a) rejections of record.

<u>Claim 12</u>

Claim 12 is rejected under 35 U.S.C. §103(a) as being unpatentable over Okada in view of United States Patent Number 6,031,992 to Cmelik et al. (hereafter referred to as "Cmelik"). Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claim 12 is not rendered obvious by Okada in view of Cmelik for the following reasons.

Applicants respectfully submit that Cmelik, either alone or in combination with Okada, fails to cure the deficiencies of Okada discussed above with respect to independent Claim 10. Specifically, Cmelik fails to teach or suggest the limitations of "wherein said digital secret is operable to be used exclusively by said processor for both encryption and decryption" as recited in independent Claim 1, and similarly recited in independent Claim 10. Consequently, since Claims 12 recites further limitations to the invention claimed in independent

Claim 10, Claim 12 is not rendered obvious by Okada in view of Cmelik. Thus, Claim 12 overcomes the 35 U.S.C. §103(a) rejections of record.

Claims 15-17 and 20

Claims 15-17 and 20 are rejected under 35 U.S.C. §103(a) as being unpatentable over Okada in view of United States Patent Application Publication Number 2004/0025036 by Balard et al. (hereafter referred to as "Balard"). Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claims 15-17 and 20 are not rendered obvious by Okada in view of Balard for the following reasons.

Applicants respectfully submit that Balard, either alone or in combination with Okada, fails to cure the deficiencies of Okada discussed above with respect to independent Claim 10. Specifically, Balard fails to teach or suggest the limitations of "wherein said digital secret is operable to be used exclusively by said processor for both encryption and decryption" as recited in independent Claim 1, and similarly recited in independent Claim 10. Consequently, since Claims 15-17 and 20 recite further limitations to the invention claimed in independent Claim 10, Claims 15-17 and 20 are not rendered obvious by Okada in view of Balard. Thus, Claims 15-17 and 20 overcome the 35 U.S.C. §103(a) rejections of record.

Claims 18-19 and 25-26

Claims 18-19 and 25-26 are rejected under 35 U.S.C. §103(a) as being unpatentable over Okada. Applicants have reviewed the cited reference and respectfully submit that the embodiments of the present invention as recited in

Claims 18-19 and 25-26 are not rendered obvious by Okada for the following reasons.

Applicants respectfully assert that neither Easter nor Klein teach or suggest the limitations of "wherein said secure cryptography unit comprises a fully integrated circuit within said processor" as recited in Claim 18 and similarly recited in Claim 25, and therefore, do not provide adequate support for the Official Notice taken in the rejection. As recited and described in the present application, a secure cryptography unit comprises a fully integrated circuit within a processor, where communication within the unit may be performed without the use of a bus (see lines 20-22 of page 18 of the present application).

In contrast to the claimed embodiments, Applicants understand Easter to teach cryptography system 63 with buses 35 and 37 coupling components of system 63, where system 63 is located outside of CPU 13 (Figure 2; col. 4, lines 22-32). As such, Easter teaches that system 63 is not a fully integrated circuit since it comprises buses 35 and 37, and also teaches that system 63 is not a fully integrated circuit within system 63 since Figure 2 of Easter teaches that system 63 is located externally to CPU 13 (assuming arguendo that CPU 13 of Easter is analogous to a processor as claimed).

Further, Easter teaches that key array 25 provides storage for public keys (col. 4, lines 63-65). Applicants respectfully assert that public keys are very different from digital secrets as claimed. Thus, Applicants respectfully assert that Easter fails to teach or suggest a secure cryptography unit as recited in independent Claim 10 from which Claim 18 depends.

Additionally, in contrast to the claimed embodiments, Applicants fail to find any teaching or suggestion in Klein of a cryptography unit comprising a fully integrated circuit within a processor as claimed. For example, assuming arguendo that logic circuit 50 is analogous to a secure cryptography unit as claimed, Applicants fail to find any teaching or suggestion in Klein that components of circuit 50 are fully integrated (e.g., communicate without a bus) as claimed. Additionally, Figure 3 of Klein shows components 51-70 coupled with arrows which Applicants understand to represent buses, and thus, Applicants respectfully assert that Klein teaches away from the claimed embodiments by showing components of circuit which use buses to communicate and are therefore not fully integrated as claimed. Further, Figure 3 of Klein teaches that logic circuit 50 is located externally to processor 36, and thus, Applicants respectfully assert that Klein further teaches away from the claimed embodiments by teaching that logic circuit 50 is *located externally to* processor 36 instead of comprising a fully integrated circuit *within* a processor as claimed (assuming arguendo that processor 36 of Klein is analogous to a processor as claimed).

Applicants respectfully assert that neither Easter nor Klein teach or suggest the limitations of "wherein said digital secret and said internal memory are fully integrated with said cryptography engine to facilitate communication without use of a bus" as recited in Claim 19 and similarly recited in Claim 26, and therefore, do not provide adequate support for the Official Notice taken in the rejection. As recited and described in the present application, a digital secret and an internal memory are fully integrated with a cryptography engine to facilitate communication without use of a bus.

In contrast to the claimed embodiments, Applicants understand Easter to teach key array 25 coupled to RSA engine 57 by bus 37 (Figure 2). Assuming arguendo that key array 25 is analogous to an internal memory as claimed, also assuming arguendo that a key of key array 25 is analogous to a digital secret as claimed, and further assuming arguendo that RSA engine 57 is analogous to a cryptography engine as claimed, Applicants respectfully assert that Easter teaches away from the claimed embodiments by teaching that they communicate via bus 37 instead of without the use of a bus as claimed. Additionally, Applicants respectfully assert that Easter further teaches away from the claimed embodiments by teaching that the keys within key array 25 are public keys as discussed above instead of digital secrets as claimed.

Additionally, in contrast to the claimed embodiments, Applicants understand Klein to teach components of logic circuit 50 coupled to encryption engine 60 by buses (Figure 3). Assuming arguendo that key register 66 or component 64 is analogous to an internal memory as claimed, also assuming arguendo that a key of key register 66 or a hardware identifier of component 64 is analogous to a digital secret as claimed, and further assuming arguendo that encryption engine 60 is analogous to a cryptography engine as claimed, Applicants respectfully assert that Klein fails to teach or suggest that the components of logic circuit 50 communicate without the use of a bus as claimed.

Moreover, as discussed above, Okada fails to teach or suggest the limitations of "wherein said digital secret is operable to be used exclusively by said processor for both encryption and decryption" as recited in independent Claim 1, and similarly recited in independent Claims 10 and 21. Consequently, since Claims 18-19 and 25-26 recite further limitations to the invention claimed in

their respective independent Claims, Claims 18-19 and 25-26 are not rendered obvious by Okada. Thus, Claims 18-19 and 25-26 overcome the 35 U.S.C. §103(a) rejections of record.

<u>CONCLUSION</u>

Applicant respectfully submits that Claims 1-26 are in condition for allowance and Applicants earnestly solicit such action from the Examiner.

The Examiner is urged to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present application.

Please charge any additional fees or apply any credits to our PTO deposit account number: 50-4160.

Respectfully submitted,

MURABITO, HAO & BARNES LLP

Dated: 10/19, 2007

BMF

Bryan M. Failing
Registration No. 57,974

Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060